UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

22850 7590 03/18/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LE, CANH	
ART UNIT	**PAPER NUMBER**
2139	
NOTIFICATION DATE	**DELIVERY MODE**
03/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/749,412	**Applicant(s)** OCHI ET AL.	
	Examiner CANH LE	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/17/2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6, 8-16, and 18-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-16 and 18-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 12/17/2007.

Claims 7 and 17 have been cancelled.

Claims 1-6, 8-16, 18-22 have been amended.

Claims 1-6, 8-16, and 18-22 have been examined and are pending.

Response to Amendment

Applicant's amended claims, see page 12, filed 12/17/2007, with respect to the 35 U.S.C.101 rejection of claims 21-22 have been fully considered and are persuasive. The 35 U.S.C. 101 rejection of claims 21-22 has been withdrawn.

Applicant's amended claims, see pages 12-13, filed 12/17/2007, with respect to the 35 U.S.C. 112, second paragraph of claims 2 and 12 have been fully considered and are persuasive. The 35 U.S.C. 112, second paragraph of claims 2 and 12 has been withdrawn.

The applicant's amendment filed 12/17/2007 necessitated the new ground(s) of rejection presented in this Office action. Therefore, applicant's arguments with respect to claims 1-6, 8-16, and 18-22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 9-15, and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A).

<u>As per claims 11, 1, 21:</u>

Claim 11:

Schneier teaches an encryption processing method for performing a_data encryption process, said encryption processing method comprising:

(a) dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs];**

(b) setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units under a condition in which the processing sequence of the encryption processing units, set in said dividing, within each group is fixed **[pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC**

mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption. Each triple-DES is fixed]; and

(c) performing an encryption process in accordance with the mixed encryption processing sequence set in the setting, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process **[pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining (TCBC) encryption. In the TCBC includes a triple-DES encryption process]**, and

Schneier does not explicitly teach a limitation of setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple-DES encryption process.

However, Lin teaches a limitation setting a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups, and setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple-DES encryption process **[abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to**

confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance". It is obvious for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Schneier by including the step of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin, pg. 11, lines 18-19].**

Claims 1 and 21 are essentially the same as claim 11 except that they set forth the claimed invention as an apparatus / a computer program rather than a method and rejected under the same reasons as applied above.

As per claims 12, 2:

Claim 12:

Lin further teaches an encryption processing method according to claim 11, further comprising setting a dummy encryption processing unit that performs the dummy encryption process, and setting one mixed encryption processing sequence by mixing the encryption processing units of a plurality of groups containing said dummy encryption processing units **[abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy"**

operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance”].

Claim 2 is essentially the same as claim 12 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claim 13, 3:

Claim 13:

Schneier further teaches an encryption processing method according to claim 11 , wherein said dividing determines a group of sequences, which can be performed independently of each other, within the original encryption processing sequence to be divided in a process of division into a plurality of groups composed of one or more encryption processing units, and performs a process for setting a group of divisions in which the sequence which can be performed independently is a unit **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DES; page 272, figure 12.2 One round of DES; Each S-box independently performs an encryption processing as a unit]**.

Claim 3 is essentially the same as claim 13 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 14, 4:

Claim 14:

Schneier further teaches an encryption processing method according to claim 11, , wherein said encryption processing unit is a single-DES encryption process,

(a) said dividing divides the original encryption processing sequence containing one or more single-DES encryption processes into a plurality of groups composed of one or more single-DES encryption processes **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs]**, and

(b) said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group of divisions by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed **[pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence**

of encryption processing in triple-DES Cipher Block Chaining encryption. Each triple-DES is fixed].

Claim 4 is essentially the same as claim 14 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

<u>**As per claims 15, 5:**</u>

Claim 15:

Schneier further teaches an encryption processing method according to claim 11 , wherein

(a) said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES encryption process which forms the triple-DES encryption process being an encryption processing unit **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs].**

Claim 5 is essentially the same as claim 15 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 19, 9, 22:

Claim 19:

Schneier teaches an encryption processing method for performing a data encryption process, said encryption processing method comprising:

(a) dividing an original encryption processing sequence into one or more encryption processing units **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs]**;

(b) setting a mixed encryption processing sequence, mixing processing sequences of the original encryption processing units included in the original encryption processing sequence **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs]**.

(c) performing an encryption process in accordance with the mixed encryption processing sequence, wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process **[pg.**

358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining (TCBC) encryption. In the TCBC includes a triple-DES encryption process],

Schneier does not explicitly teach adding a dummy encryption processing unit that performs a dummy-single DES process as a dummy encryption process that is unnecessary for the original processing sequence and that corresponds to said encryption processing unit, and setting the number of dummy single-DES processes to a multiple of 3 corresponding to the triple-DES encryption process.

However, Lin teaches adding a dummy encryption processing unit that performs a dummy-single DES process as a dummy encryption process that is unnecessary for the original processing sequence and that corresponds to said encryption processing unit, and setting the number of dummy single-DES processes to a multiple of 3 corresponding to the triple-DES encryption process **[abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance". It is obvious for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Schneier by including the step of Lin because it would perform the DES operation and the benefit gained in DPA attack resistance **[Lin, pg. 11, lines 18-19].**

Claims 9 and 22 are essentially the same as claim 19 except that they set forth the claimed invention as an apparatus / a computer program rather than a method and rejected under the same reasons as applied above.

<u>As per claims 20, 10:</u>

Claim 20:

Schneier further teaches an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process **[pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3DESs]**, and

Lin further teaches setting a dummy encryption processing unit as a single-DES encryption process **[abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to confuse analysis of a power signature… The number of dummy look-ups**

performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance".

Claim 10 is essentially the same as claim 20 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) and further in view of **Kocher et al.** (US 2001/0053220 A1).

<u>As per claims 16, 6:</u>

Claim 16:

Schneier and Lin teach the subject matter as described above.

Schneier teaches an encryption processing method according wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process as described in claim 11.

Schneier and Lin do not explicitly teach a random number generation process including a conversion process by three single-DES processes and setting the triple-DES encryption process as a random-number generation process in one of the groups of divisions.

However, Kocher teaches a random-number generation process and said encryption processing method further comprises the steps of forming a random-number generation process as a process including a conversion process by three single-DES processes and setting the triple-DES encryption process as a random-number generation process in one of the groups of divisions **[par. [0006]; "triple DES (a cipher constructed using three applications of Data Encryption Standard using different keys) can resist all feasible cryptanalytic attacks, provided that attackers only have access to the standard inputs to and outputs from the protocol"; par. [0008], lines 6-8; a key management devices introduce randomness].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Schneier and Lin by including the step of Kocher because it would provide unpredictability into their internal state **[Kocher, par. [008]].**

Claim 6 is essentially the same as claim 16 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above

Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) and further in view of **Kaminaga et al** (US 2002/0124179 A1).

As per claims 18, 8:

Claim 18:

Schneier and Lin teach the subject matter as described above.

Schneier and Lin do not explicitly teach storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from.

However, Kaminaga teaches storing processing results in a memory for storing processing results of the encryption processing units which form the mixed encryption processing sequence in such a manner as to be capable of identifying which encryption processing unit the processing results are obtained from **[abstract, par. [0039], lines 7-10; "processed by an encryption process (step 503). The result Z obtained in the process performed in step 503 is stored on a RAM (step 504)"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the encryption processing method of Schneier and Lin by including the step of Kaminaga because it would detect an erroneous operation during encryption processing is that before the output of the encrypted result, the ciphertext result, the ciphertext is again decrypted to a plaintext and compared with the original text, and when they are identical to each other, the ciphertext is output and when they are different, the result of the encryption-process is not output to the external device **[Kaminaga, par. [0014]].**

Claim 8 is essentially the same as claim 18 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 20030002664 A1 to Anand, Satish N.;

US 6658569 B1 to Patarin; Jacques et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
March 2, 2008

/Matthew Heneghan/

Primary Examiner, Art Unit 2139